ICS-CERT ADVISORY

ICSA-12-079-01—MICROSOFT REMOTE DESKTOP PROTOCOL MEMORY CORRUPTION VULNERABILITY

March 19, 2012

OVERVIEW

ICS-CERT is aware of a public report of a Remote Desktop Protocol (RDP) vulnerability with proof-of-concept (PoC) exploit code affecting multiple Microsoft Windows operating systems. RDP is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to another computer. In a control system environment, this protocol is typically used for remote access.

Security researcher Luigi Auriemma coordinated the release of this information through the Zero Day Initiative (ZDI).[a] Microsoft[b] has issued a patch for this vulnerability that is available on their update website or automatically if automatic updates are turned on in a system. Though this report is not industrial control system (ICS)-specific, the results of successfully exploiting this vulnerability are far reaching into the ICS environment.

AFFECTED PRODUCTS

For a list of all affected Microsoft products, please visit the Microsoft Security Bulletin:

http://technet.microsoft.com/en-us/security/bulletin/ms12-020

IMPACT

Successful exploitation of this vulnerability in the control systems environment could lead to system processes freezing and potentially allow remote code execution.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

a. http://www.zerodayinitiative.com/advisories/ZDI-12-044/ , website last accessed March 19, 2012
b. http://technet.microsoft.com/en-us/security/bulletin/ms12-020 , website last accessed March 19, 2012

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The vulnerable RDP implementation does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending a sequence of specially crafted RDP packets to Port 3389/TCP.

CVE-2012-0002[c] has been assigned to this vulnerability. According to ZDI, a CVSS V2 base score of 10.0 has also been assigned.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploits are known to target this vulnerability.

DIFFICULTY

An attacker with a low skill level would be able to exploit this vulnerability.

MITIGATION

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Audit your network for systems using RDP for remote communication and either disable the service if unneeded or install the available patch from Microsoft. Users may need to work with their vendors to confirm that this patch will not affect system processes.
- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

c. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0002, website last accessed March 19, 2012

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[d] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.

d. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed March 19, 2012.